Arolygiaeth Ei Mawrhydi dros Addysg a Hyfforddiant yng Nghymru
Her Majesty's Inspectorate for Education and Training in Wales

ICT usage policy

Information sheet

Information box

For further advice contact: InformationTechology Security Officer (ITSO)
ITSO@estyn.gov.uk

This policy and its associated procedures are agreed by Estyn's management and Trades Unions

Date of publication: October 2018
Planned review start date: March 2020

Version control

Version	Author	Date of issue	Comments
1.0	Phil Sweeney	January 2014	Draft for staff comments
2.0	Information Governance Group	14 April 2014	Review completed
3.0	Information Governance Group	February 2017	Clarified definition of 'ICT service desk' with contact details for Westgate. Clarified that you should change your password immediately after any maintenance which has required you to share it. Included references to our terminal Services client for business continuity. For guidance please see: https://vir.estyn.gov.uk/vir/Business%20Continuity/Business%20Continuity%20Documents/Forms/AllItems.aspx Include references to tablets as they are now used for business and as such are covered by the policy. Removed requirement for a PIN number to access your phone voicemail. Amended some points to exempt Estyn staff in certain situations if they are involved in moving equipment or acting in a system support role. Included requirement that personal data only be held on encrypted external storage devices.

			Clarified our stance on not using Estyn equipment connected to the Estyn network to access personal email and social networking sites. Clarified Estyn's wireless networks and how they should be used. Included an FAQ (Q10) with details on our policy on downloading apps to Estyn smartphones.
4.0	Information Governance Group	October 2018	Updated with references to the new General Data Protection Regulations rather than the Data Protection Act. Password requirements have been tightened and further guidance included. The ITSO must approve: • any software to be installed on Estyn IT • any new systems designed to store personal information. These should also undergo a security assessment. Estyn no longer offers staff the use of a 'kiosk' machine un-connected to the network. Further clarification on personal use of Estyn IT. Clarification and explanation over using personal IT to log on to the Estyn network, in cases when this may be required for disaster recovery or business contiuity.

Equality Impact Assessment

A business rationale assessment has been carried out and this policy contributes to Estyn's strategic objectives and delivery principles.

In accordance with Estyn's Equality Impact Assessment, an initial screening impact assessment has been carried out and this policy is not deemed to adversely impact on the grounds of the nine protected characteristics as laid out by the Equality Act 2010.

Contents

1 Introduction

1.1 The information and communication technology (ICT) network, equipment and official telephones (hereafter referred to as the "ICT systems") of Estyn are provided to support its business activities. The rules within this policy are designed to ensure that use of the ICT systems is efficient and secure and does not expose Estyn to major business or legal risks.

1.2 The 'ICT service desk' is your first port of call for all issues and enquiries surrounding ICT systems use within Estyn. Our current ICT service desk provider is Westgate IT. Their contact details are 0330 2020 369 or support@westgateit.com

1.3 This document sets out the rules regarding acceptable use by ALL workers that make use of the ICT systems within Estyn. The rules apply equally to consultants and contractors who are granted access to the ICT systems and their contracts with Estyn will reflect this requirement.

1.4 Some limited personal use is allowed under the conditions set out in these rules, but each user is required to behave in a responsible manner when using the ICT systems. Estyn staff should also be aware that conduct matters relevant to the use of ICT systems are covered by Estyn's Discipline Policy.

1.5 These rules may be updated from time to time and the policy will be reviewed regularly. Changes to the rules will be publicised via SharePoint and other corporate communication channels.

1.6 Estyn staff should also be aware of the following related documents:

Estyn's Discipline Policy
Estyn's Data Protection Policy
Estyn's Information Assurance Policy
Estyn's Health and Safety Policy
The Human Rights Act, 2000
The Computer Misuse Act, 1990 (and Part 5 of the Police and Justice Act 2006)
The Data Protection Act, 1998 amended by The Data Protection Act. 2003
The Regulation of Investigatory Powers Act, 2000
The Freedom of Information Act, 2000 and 2005
The Official Secrets Act, 1989
The Investigatory Powers Bill, 2015
General Data Protecton Regulation (GDPR) 2016

1.7 Any information stored on or which is communicated using the Estyn ICT systems is not private and may be checked (e.g. read, listened to or copied), without notice, for the following purposes:

i. for quality control and staff training purposes;
ii. to help maintain compliance with practices or procedures set out in law;
iii. to establish facts and protect the interests of Estyn;
iv. to prevent unauthorised use of ICT systems;

v. to prevent inappropriate/offensive media being stored on, or communicated using the ICT systems;
vi. to assist with any investigation or action proposed by lawfully authorised investigating or regulatory bodies (e.g. Police); and
vii. to comply with access to information obligations under, for example, the General Data Protection Regulation and the Freedom of Information Act.

1.8 Estyn also reserves the right to make and keep copies of all information, (including but not limited to telephone calls, emails and data documenting use of the telephone, email, Internet systems or removable media) for the purposes set out above, and if it sees fit, to use the information in disciplinary proceedings against employees.

2 Health and safety

2.1 Advice on workstation assessment and any issues regarding accessibility is available from Estyn's Health and Safety Officer and the Human Resources team.

3 Care of ICT equipment

3.1 You are responsible for taking care of the ICT equipment you are using. Such equipment will be procured and disposed of through central arrangements. Personally allocated equipment such as laptops or mobile phones must not be passed on to colleagues.

3.2 Computer workstations located in the office will be automatically powered-down at a scheduled time each day (currently 19:00). However, to avoid potential loss of data staff are advised to always log-off and shut down their computer before leaving the office.

3.3 Particular care must be taken regarding CDs, USB memory sticks and other removable media. These items are mechanisms for virus transmission and potential loss of data. For data security purposes, do not retain information on portable media for longer than required to meet business needs.

3.4 If equipment in your charge (including removable media) is lost or damaged you must report it immediately to the Information Technology Security Officer (ITSO) and to your line manager. Please be aware that individuals may be charged for negligent loss or damage, and may also be subject to disciplinary action.

3.5 You should avoid:

i. eating or drinking over a computer;
ii. trailing wires where people might trip over them; and must not
iii. attempt to open computer and telephony equipment casings unless guided to do so by the ICT Service Desk.

3.6 Only data stored on the shared network drives (e.g. SharePoint) and the user's Y Drive will be automatically backed up when the computer is connected to the Estyn network, either in the office or connected remotely via the VPN.

3.7 The C: Drive or Desktop on computers should not be used for storing information as the C: Drive is not backed up and information may be accessed inappropriately by someone who gains access to a user's machine. N.B. Information stored in the Y Drive is more secure and is available off-line for laptop users. The Y: Drive should only be used for short term storage and weeded rountuniely.

4 User identification

4.1 Access to ICT systems is allocated via a unique username, which is protected by password. It is a disciplinary offence to log on as another user or access any ICT systems that you have not been authorised to access, unless you are engaged in diagnosis in a systems support role, or acting under the instructions of our technical advisers.

4.2 You are responsible for any network activities that occur while your account is logged in to the system. Therefore you must not allow anyone else, e.g. a visitor, a contractor or another member of staff to use your username and password. On occasions when username and password are required by ICT Service Desk, for example for technical support purposes, you should change the password the next time you log on to your machine and the Estyn network.

4.3 Normally, you should log on to your account from only one computer at a time. If it is essential that you log on to your account simultaneously from two or more computers, for example, as part of a fault resolution exercise or when presenting information at a meeting away from your normal work space, you must ensure that the computer you are not using has been screen-locked.

4.4 At all times and especially as part of the process of terminating your employment or engagement with Estyn, you and your line manager are responsible for ensuring that any work related information of continuing value that is not already stored on the shared network drive, including any relevant emails within a user's Estyn account, is transferred to the network. The manager will be responsible for ensuring that any information retained is managed in line with GDPR requirements.

5 Passwords and PINs

5.1 Passwords must be a minimum of twelve characters and must contain at least one Lowercase letter, one upper case letter and one number or special character (! % @ etc). The lockout threshold, the number of tries before the account locks for 15 minutes, is set to ten attempts. Password history setting is set at twenty four in order to prevent reuse of old passwords.

5.2 You must not share your password or any PIN or ask a colleague to divulge theirs. Doing so is considered a serious disciplinary offence. The only exception is the maintenance case set out in para 4.2 above. After maintenance you should change your password immediately.

5.3 Your password must not be familiar and easy to guess. It should not therefore contain family names or place-names. A word or mnemonic known to you allied with numbers is usually regarded as a 'strong' password. (An 8-alpha plus 2-numeric password is regarded as 'very strong').

5.4 You must not allow any passwords to Estyn systems to be entered automatically by "auto-complete" facilities or macros.

5.5 If you believe your password or PIN has become known to someone else, you must immediately change it.

5.6 If you have forgotten your password you will need to contact the ICT Service Desk (your line manager will be required to confirm the request by email) before it can be reset. Homeworking staff may have to answer security questions to validate identity before the reset can take place. Please note, if you are unable to provide correct answers to your security questions, or do not have those questions set up, you will not be able to reset your password until your identity has been verified, e.g. by your line manager or the IT Security Officer.

6 Systems security

6.1 Software installed on Estyn PCs, laptops and other devices must be approved by the ITSO. Estyn will only provide technical support for equipment and software that it has issued and installed.

6.2 To avoid virus or malware contamination, personally-owned ICT equipment (e.g. laptops, memory sticks, mobile phones or digital cameras) must not be connected to the internal Estyn network or ICT equipment. Data may be transferred from devices obtained from providers/partners where assurances, preferably written, have been received from the provider/partner regarding their use of appropriate anti-virus software – if in any doubt then please contact the ITSO for advice.

6.3 You must not attempt to disable any anti-virus software or any other software that has been loaded on to your computer unless instructed to do so by the ICT Service Desk.

6.4 Estyn makes use of a variety of different computer applications to support business activities. These range from corporate systems (e.g. Cygnum) through to spreadsheets managed and used by individual members of staff. Each application must have a System Owner (who will also be the Information Asset Owner) who carries overall responsibility for its integrity and defines the criteria under which the

data can be accessed or altered (for further information please refer to Estyn internal guidance on electronic records management).

6.5 The Information Asset Owner is responsible for ensuring that any personal data is handled in accordance with the Data Protection Act, GDPR and Estyn's information governance policies. In order to do this, Information Asset Owners should liaise with the ITSO.

6.6 Each user of the ICT systems is personally responsible for any breach of these rules and for taking action to prevent breaches of information security. All staff are personally responsible for making themselves aware of the content of the rules contained in this document, and should be aware that by logging on to the corporate network they agree to be bound by the terms of these rules.

6.7 Any observed or suspected security weaknesses or threats to the ICT systems must be reported to the ICT Service Desk and the ITSO. Other security matters should be reported to Office Services.

6.8 Viruses, Ransomware,Trojans and Worms can do considerable damage to systems and may affect the ability of Estyn to access its information. Common sources are:

i. email attachments;
ii. external networks;
iii. the Internet; and
iv. file sharing with external PCs using CD-ROM or other removable media.

6.9 If you are notified by an outside body that a computer virus may have entered the Estyn network then you must inform the ICT Service Desk immediately. However, a large number of hoax virus warnings are often in circulation and overreacting to them can cause as much of a nuisance as some real viruses. Therefore you should not circulate a virus warning, e.g. via email, to any other member of staff; please refer them to the ICT Service Desk.

6.10 If you receive a suspicious email with an attachment you must always forward it unopened to the ICT Service Desk for checking.

6.11 In the event of a virus outbreak, users must follow the instructions given by the ITSO or ICT Service Desk to protect Estyn systems. Failure to do so may result in disciplinary action.

6.12 All new systems that are intended to store any personal information, and/or send and receive information electronically from an external source must undergo a security assessment and be cleared with the ITSO prior to implementation.

6.13 The deliberate introduction of a damaging virus is a criminal offence under the Computer Misuse Act 1990.

7 Software protection

7.1 Only software obtained through centrally agreed arrangements is allowed on the Estyn network.

7.2 Requests for the installation of any new software must be made by email to the ICT Help Desk. In the case of new licensed software, you will need to supply evidence that the budget holder has approved expenditure and Estyn has purchased a license. Existing licensed software can be installed on demand providing we have sufficient licenses available.

7.3 Copying existing software is not allowed as it may infringe copyright. If another copy of the software is required you must contact the ICT Service Desk.

7.4 Unauthorised software identified through routine audits will be removed by the ICT Service Desk and disciplinary proceedings may be taken against the employee concerned

8 Personal use of Estyn ICT systems

8.1 All ICT equipment, telephones and mobile devices are provided for the purpose of undertaking Estyn business, and staff should therefore use them to carry out work related to their role within the organisation. They are not normally intended for conducting communications on personal matters with contacts within or outside Estyn, whatever the nature or purpose of that communication.

8.2 However, it is recognised that personal communications are sometimes necessary during the working day. A limited amount of personal email, Skype, Skype instant messaging or telephone communication is therefore allowed, provided:

i. it is restricted to non-working time, except in emergencies, and does not interfere with official duties;
ii. it will not embarrass Estyn or its staff nor cause any reputational damage to Estyn (this includes comments posted to any social networking sites);
iii. it does not affect the performance of the ICT systems;
iv. there is no infringement of copyright or other unlawful activity; and
v. it is not associated with any personal profit or business profit-making with any external organisation.

(Further guidance on use of email and telephones is provided within later sections of this policy.)

8.3 Similarly, a limited amount of personal access to the Internet during non-working time (i.e. lunchtimes and before/after working hours) is also allowed, subject to the conditions laid out in paragraph 8.2. However, staff should be aware that personal

use of official ICT systems is at management discretion and is not an automatic right. (See section 12 for more guidance on Internet usage.)

8.4 You must ensure all data, including that stored on network drives, local hard drive and removable media, complies with legal requirements such as the Freedom of Information Act, the Data Protection Act and GDPR. You must not store any information that is not related to carrying out the business of Estyn, for example details of non-work related contacts, information relating to personal financial transactions or any other non-work related matter. If in any doubt, please contact the ITSO.

8.5 Personal, non-work related documents or files stored on any drive are stored at your own risk.

8.6 Non work-related media files (e.g. music, video, games, movie clips, films, animations and images) should not be stored on the network. Any non-work-related media files that are found on the Estyn IT systems may be deleted without notice.

8.7 You are responsible for ensuring that media files do not infringe copyright. If you receive one of these file types (e.g. in an email from a friend) you must delete it immediately from the system. You must not store the file or the email containing it on the network drives or the C: Drive of your computer or forward it onto anyone else, including your own personal email address, unless you are reporting the matter to the ICT Service Desk as a potential breach of the ICT usage rules.

8.8 You must not under any circumstances rename a file to hide its contents e.g. renaming a .jpg image file to .xls so that it appears to be a spreadsheet. Similarly, you must not attempt to conceal a file's contents by embedding it in another file – e.g. pasting image files into a Word document.

9 Use of electronic mail (official and personal)

9.1 All emails that enter/leave the Estyn network are scanned for viruses, spam and inappropriate images. It is not easy to define what constitutes an inappropriate image but examples include any picture that includes full or partial nudity or that depicts violence or discrimination towards others or which could be construed as inciting racial or religious hatred. This includes images that are classed as 'soft porn' e.g. Page 3 pin-up type pictures. Staff need to be aware that images that are seen by some as humorous can cause offence to others.

9.2 It will not always be appropriate to communicate by email and you must always consider whether there is a more suitable method. Consider whether circumstances dictate a need to preserve confidentiality, whether discussion of sensitive issues should be communicated face to face or whether sharing a large attachment with a group of people is appropriate.

9.3 **The illusion of "privacy".** Between the originator of an email, Instant Message, etc. and its recipient(s) a message may be recorded several times. Staff need to be aware that copies may be retrieved and read by persons other than the intended recipients (e.g. to fulfil subject access requests under the Data Protection Act or Freedom of Information Act).

9.4 **Ethical issues.** Due to the lack of privacy it is important that nothing is contained within an email which could potentially be considered as offensive to the recipient or any other person.

9.5 **The potential legal liability.** Email carries legal risks (called "vicarious liability") for the user and Estyn arising from the accidental or deliberate infringement of laws including (but not limited to):

- defamation;
- obscene or blasphemous material;
- protection of children;
- discrimination/harassment, human rights;
- unwanted contract formation;
- copyright designs and patents, data protection and privacy;
- computer crime e.g. Computer Misuse Act, Telecommunications Acts, Regulation of Investigatory Powers; and
- trademarks

You may inadvertently commit an offence under one or several of the following:

- Human Rights Act 2000;
- Computer Misuse Act 1990;
- Data Protection Act 1998;
- General Data Protection Regulation 2016;
- Regulation of Investigatory Powers Act 2000;
- Freedom of Information Act 2000 and 2005;or
- Official Secrets Act 1989.

all of which apply in this context.

9.6 If you have any queries about the content of an email (received or to be sent) you must consult either your line manager, Human Resources or the ITSO. If in doubt, do not send the email.

9.7 Generally, you should not use an email disclaimer for work-related email. A disclaimer **must** be included for all personal (non work-related) emails sent outside of Estyn.

The wording of the disclaimer is:

"Any of the statements or comments made above should be regarded as personal and not necessarily those of the Estyn, any constituent part or connected body."

"Dylai'r datganiadau neu'r sylwadau uchod gael eu trin fel rhai personol ac nid o reidrwydd fel datganiadau neu sylwadau gan Estyn, unrhyw ran ohono neu unrhyw gorff sy'n gysylltiedig ag ef."

9.8 Inappropriate or suspicious emails (such as unsolicited emails requesting personal information) must be forwarded to the ITSO. Exercise caution when opening attachments to emails that you receive unexpectedly or from an unfamiliar sender. If in doubt contact the ITSO.

9.9 Except where prior permission has been obtained from the ICT Service Desk you must not use images or graphics (e.g. 'smileys') within signatures or salutations at the end of an email to an external address. The only exceptions are those logos and strap lines approved by Estyn as part of its communication protocols.

9.10 There are several practical steps you can take to avoid a situation that may cause you to be in breach of Estyn's policy in relation to email:

- Do not use the Estyn ICT systems in a way that could cause offence to others. Jokes or comments that may seem innocent to one person can cause serious offence to another.

- Keep the number of personal emails you send to a reasonable limit (no more than a handful of messages a week) and unless urgent, avoid sending them during working hours. Always attach the personal disclaimer to such emails.

- If you have a personal email address you should give this out to your friends/family for personal correspondence rather than your business email address.

- If friends do know your Estyn email address, discourage them from sending you images or emails that breach the ICT usage rules. Remind your friends/family that all emails entering the network are scanned for viruses, spam and inappropriate images and that personal email traffic should be kept to a minimum.

10 Web-based email

10.1 Generally, you should not use equipment which is connected to the Estyn network to log on to any private or commercial email system, for example, Internet (web-based) email services such as Hotmail or Gmail due to the increased security risk. When on inspection or other 'remote' service it is recognised that staff may have access to the Internet via wireless networks and might want to catch up on personal email – this is considered as acceptable use, although staff should take care to not open any suspicious emails or attachments which might contain viruses, etc.

11 Out-of-office messages and auto-signatures

11.1 When using the Estyn email system (Outlook), you must not automatically forward emails from your Estyn email account to another email account. The main reasons for this are that you could inadvertently send protectively marked information out of the network and that you could set up an email loop that crashes the email system.

11.2 You must not create an Out-of-Office rule that automatically responds to every email that you are sent. If you are away from the office for an extended period of time, your line manager can periodically ask the ICT Service Desk to reset your message so that people who have previously emailed you are reminded of your absence.

11.3 Your Out-of-Office message and auto-signature must only be used to provide alternate contact details for work-related purposes. You must not include personal contact details e.g. personal mobile phone and personal email addresses in your Out-of-Office message for the benefit of others e.g. friends and family who might communicate with you via your business email address.

11.4 All staff must use bilingual Out-of-Office messages and auto-signatures. Further information is available from the Communications team.

12 Use of the Internet

12.1 Access to the Internet will usually be via an onward connection – i.e. you will connect to the Estyn network and then access the Internet via the Estyn Internet gateway. Remote users might connect to the Internet by other means, which could involve a local wireless network in a school or other institution. Estyn's IT usage rules should still be followed even though the communication medium may be owned and operated by others.

12.2 Internet access is provided for the primary purpose of undertaking Estyn business. The facility may also be used by staff for personal reasons providing that this does not interfere with the need to get the job done nor embarrass Estyn or its staff. You will be expected to restrict your personal use to within reasonable limits as detailed below.

12.3 Estyn's office at Anchor Court has two wireless networks:

Estyn	To be used by Estyn staff on official business
EstynGuest	To be used by visitors or personal devices.

12.4 You may shop over the Internet for personal items but this must not be undertaken in any way that would imply that the activity is being carried out on behalf of Estyn as this could bring the organisations into disrepute.

12.5 In particular if you are buying or selling items outside of Estyn, you must not use your Estyn email address, telephone number or postal address for contact and delivery

purposes. For purchasing of official items over the Internet, please contact the Finance Team.

12.6 All personal Internet use is carried out at your own risk. Estyn accepts no liability for any loss or damage suffered by any user arising from personal use of the Internet. Staff should familiarise themselves with techniques of browser memory clearance so that their personal financial integrity is protected.

12.7 You must not access web sites or chat-rooms that are offensive or inappropriate to the workplace.

12.8 You must not access any social networking sites (Facebook, Twitter, Bebo, MySpace, MSN etc.) using Estyn systems, for non-work-related purpose during working hours. Estyn's Social Media Policy and Guidelines sets out how you should conduct yourself online, whether in work or in personal time, using work or personal IT devices.

12.9 You may use your own personal mobile phone or tablet to access social networking sites but only over the appropriate wifi account and during lunch or rest breaks.

12.10 Estyn automatically restricts access to certain categories of web site. However, the fact that access to a site has not been restricted should not be interpreted as it being approved to view. Should you accidentally access an offensive web site or chat room, you must leave the site immediately and notify your line manager and the ITSO of the incident.

12.11 If you require access to a blocked site for legitimate work-related reasons, a request must be made to the ITSO. You will be expected to provide a brief business case to explain why access is necessary.

12.12 You must not try to download software from the Internet as this can affect or damage the performance of the network. Certain web sites offer to download the latest versions or upgrades to existing software as soon as you visit them. You must always indicate "No" to such offers unless otherwise advised by the IT Service Desk. Please be aware that systems might be damaged by unauthorised software downloads and this may result in disciplinary action.

12.13 Should you require access to software from the Internet then you must submit an email request to ITSO to gain authorisation. It may also be necessary to arrange for the purchase of licences for the software.

12.14 You must not put on the Internet any material, which incites, encourages or enables others to gain unauthorised access to Estyn ICT systems.

12.15 Staff may only use Estyn equipment to contribute to social networking or blogging sites for work-related purposes. Staff should also be aware that if they use such sites outside of work, they must not behave in a way that brings either colleagues or the organisation into disrepute. Further guidance is provided in Estyn's Social Media Policy and Guidelines.

13 Use of official telephones

13.1 All official telephones must be used in a professional manner, appropriate to the business of Estyn.

13.2 Personal use of telephones must be consistent with the rules stated in para 8.2. Calls must be kept to a minimum and dealt with as briefly as possible so that the use of the lines for official business is not unduly restricted.

13.3 Guidance on bilingual greetings and messages is available from the Secretariat, Corporate Services.

14 Mobile telephones

14.1 Mobile phones are supplied for business purposes only to enable staff on external duties to conduct core business. Personal use of Estyn mobile phones is not generally allowed, otherwise there may be personal tax implications. However, use in an emergency situation or to notify family or friends to prevent unnecessary distress or worries, e.g. during travel delays, is acceptable.

14.2 Mobile telephones remain attractive items and can be a target for thieves and therefore should always be used discreetly.

14.3 All available security devices such as key-pad locking codes and pin-codes must be used to prevent unauthorised use in the event of loss or theft.

14.4 When offsite, phones must not be left unattended in jacket pockets, handbags or luggage but must be carried and concealed on the individual.

14.5 In the event of theft or loss, the mobile phone user is responsible for contacting the ITSO or Office Services to arrange a call bar with the network provider and remote ‘data wipe’ as soon as possible. The user must also inform the police and obtain a reference number (crime number/lost property number). The user may be held responsible for paying the full cost of a replacement handset depending on the circumstances of the loss.

14.6 If you are driving and using a mobile phone, you must adhere to Estyn’s Policy for driving as part of official duties. It is unsafe and illegal to use a hand-held mobile phone whilst driving a vehicle. Payment of any fine will be the responsibility of the individual. Making or receiving a call, even with a hands-free phone, can reduce your concentration and could lead to an accident. For this reason Estyn recommends that mobile phones should not be used whilst driving; switch off your phone, use a message service or let a passenger make or answer a call.

14.7 Employees should be aware that mobile telephones can be disruptive. Personal mobile phones should be turned off or set to “silent” or on low volume ringtone during working hours.

14.8 Mobile phones emitting radio waves above a certain level has led to public concern about the possible impact on health. Research findings to date are not conclusive, although some point to changes in brain activity caused by prolonged use of mobile phones. For this reason, a precautionary approach is recommended until more research findings become available. You can minimise your exposure to radio waves by limiting the use of the mobile phone and by keeping your calls as short as possible.

15 Delegated working

15.1 It is recognised that there are times when staff may need to access a colleague’s calendar or mailbox, either on an on-going basis (e.g. Executive Assistants) or just occasionally to cover periods of staff absence.

15.2 Personal login details should not be shared with others; there are ICT facilities that allow you to access calendars and mailboxes without having to share login information.

15.3 Ongoing, delegated access to a colleague’s calendar and mailbox may be requested through your line manager to the IT Service Desk as a support request in the normal way.

15.4 Staff who simply need to allow colleagues to monitor incoming email or calendar entries while they are out of the office should set their Outlook permissions to allow this. For more information on setting permissions contact the IT Service Desk.

16 Security matters while working remotely

16.1 When working remotely, you must take sole responsibility for protecting the assets entrusted to your safekeeping. Whilst personal safety is paramount, you must make all reasonable endeavours to ensure that opportunities for theft/loss of information and equipment is minimised at all times:

i. Laptops, tablets and mobile phones must use all available security protection such as passwords, keypad locking and PIN codes to prevent unauthorised access.
ii. Laptops, tablets and mobile phones must be stored in a secure location overnight – preferably, use lockable desk drawers or cupboards, where available.
iii. Avoid leaving ICT equipment unattended during transit.
iv. Whenever possible, carry portable equipment as hand luggage.

v. If it is necessary to leave equipment in a vehicle, ensure that it is locked away and out of sight. However, equipment must not be kept in the vehicle overnight.
vi. Avoid creating temptation – be discrete in using and storing ICT equipment.

16.2 Data backups are carried out automatically when you connect to the ICT network. If you are unable to connect to the network e.g. for technical reasons, remember that any information on your laptop will not have been backed up since the last time you were logged-on to the network. If it is important, copy the information to an external storage device, e.g. Estyn-issued encrypted data stick (an encrypted stick must be used in instances where personal data is being stored), and store securely, i.e. away from the laptop.

16.3 If you lose your Remote Access Key Fob (RSA fob) you must inform the ITSO at once.

17 Travelling

17.1 The greatest risks when working whilst travelling are theft, loss, overlooking and eavesdropping. You might often be at locations offering low levels of privacy and it is essential that you maintain a high level of vigilance.

17.2 For your own safety, avoid using your equipment in a busy public place, as you may become a target for thieves. You should aim to minimise the amount of time you carry your laptop (or other portable device) around in public. Specialist laptop cases may draw attention to their contents, so consider carrying your laptop in a briefcase or rucksack to deter casual thieves.

17.3 If you do have to use your equipment in public ensure that care is taken to avoid the risk of being overlooked/overheard e.g. whilst speaking on a mobile phone. Be aware that onlookers can view data displayed on laptop screens in public places. You must ensure you are discreet and never leave your laptop or other device, e.g. smartphone, unattended.

17.4 Equipment such as laptops and mobile phones must be physically protected against theft especially when left, for example, in cars and other forms of transport, hotel rooms, conference centres and meeting places. Where possible, equipment must be physically locked in these situations. Equipment carrying sensitive information, e.g. marked ‘Official – Personal’, must not be left unattended.

18 Working at home

18.1 ICT equipment provided by Estyn for use in the home must only be used by Estyn staff.

18.2 For security reasons, you are advised to not use your *own* ICT equipment for Estyn business. Corporate Services staff who might occasionally need to work from home should request a 'temporary' laptop from Office Services. In a Disaster Recovery or business comtinuity exercise then staff may access systems using a terminal services client downloaded to their own equipment. Estyn recognises that it cannot control the use of personal equipment but it can hold staff to account if Estyn data is lost or shared inappropriately. Therefore, if you do use your own personal equipment for business purposes, you should comply with all of the following:

i. Your computer must be **secure against virus infection** – you must install:
   - antivirus software (with the latest updates);
   - a personal firewall;
   - anti-spyware; and
   - the latest operating system patches.

ii. You must **not work on sensitive** information.

iii. The information **must be de-personalised** while on your PC e.g. remove any references to people and organisations.

iv. The information **must not be accessed by anyone else**. Therefore, when you have finished working with it, you must transfer it back to the corporate network (e.g. by email) and then take steps to remove the information from your computer including deleted items from the recycle bin, and clearing your browser cache.

19 Working overseas

19.1 The security threat while working overseas is generally greater than in the UK, i.e. there may be a greater threat from eavesdropping and interception. You must contact the ITSO prior to taking any Estyn ICT equipment overseas.

19.2 When travelling abroad, only take your ICT equipment with you if you really need to and only take the information that is necessary for the job in hand. Delete other information as soon as it has been used and copied/backed up to the network. If possible, do not take any protectively marked information with you on the hard disk. If you do work on protectively marked material, copy it back to the network as soon as possible and delete it from the hard disk.

19.3 Do not take any protectively marked or commercially sensitive information with you unless it is essential for the purposes of your visit. Before you leave you must tell the ITSO if you need to take this type of information with you. The ITSO will be able to offer advice on how to protect the material when travelling, and during your stay.

20 Airports

20.1 Obey all port of entry instructions with regard to your ICT equipment even if it would cause you to be in breach of the Estyn IT Security and Usage Policy. For example, if an immigration official tells you to start up your computer and divulge your password then do so. However, you should change your password as soon as it is safe to do so and inform the IT Security Officer of the incident as soon as you are able.

20.2 When going through airport scanners, try to avoid a situation where your laptop bag emerges from the luggage scanner before you have walked through the security checks. (There have been instances where thieves have seized laptop bags from the conveyor belt before the owner has been able to pick the equipment up.)

20.3 You may be asked to start up your equipment at airline security checks. Ensure that you have a full battery before starting your journey. If your laptop does not start, it may be confiscated.

20.4 All ICT equipment must be carried as hand luggage.

20.5 During a time of heightened airport security it may not be possible to take any equipment through as hand luggage and in this case you will need to put your ICT equipment in the hold.

20.6 If the ICT equipment has been out of your care you must advise the ITSO before you reconnect the equipment to the corporate network (either directly or remotely).

21 Protection of information

21.1 You must lock your screen when you leave your computer unattended, even if you only leave it for a matter of minutes (use CTRL-ALT-DELETE to do this). Desktop computers will time-out after 20 minutes (i.e. auto screen lock) to limit risk of unauthorised access if no activity has taken place. Activity is defined as a mouse click or key stroke.

21.2 Laptop users are able to set their own auto screen lock timings, including disabling the auto screen lock. While the auto screen lock is disabled the computer must not be left unattended at any time. Note that the laptop will return to its default setting when re-booted.

21.3 If you believe someone has accessed your network account without appropriate authority you must inform your line manager and the ITSO immediately.

21.4 When accessing or processing sensitive information you must take all reasonable precautions to ensure that others cannot view your screen – remember your screen may be more easily overlooked than a sheet of paper on your desk.

21.5 If you need to hold sensitive information on CD-ROM, USB pen-drive or other removable media then it must be stored securely when not in use. Personal data must only be stored on an encrypted device. Information held on removable media should be deleted once it is no longer required and/or has been transferred to permanent media.

21.6 You should never divulge information that could compromise system security to third parties without having first verified their identity and ascertained why they need this information. The guiding principle is: Does this person need to know this to do their job? This includes details of Estyn's ICT systems and software applications or details of the format of your network username.

21.7 If you are contacted by telephone you must ensure you are aware of the identity of the caller before discussing Estyn official business. This is particularly important should you be discussing information related to the corporate ICT systems or information that is sensitive or has a protective marking.

21.8 Care must be taken when using mobile phones or Skype not to discuss sensitive information, for example safeguarding issues, disciplinary matters, sensitive reports or investigations. Calls made on mobile phones and Skype are very insecure. Conversations in public places can be overheard and scanning equipment can pick up signals and intercept text messages and calls made. Landlines are less insecure; however, highly sensitive issues are best discussed in-person, where possible.

22 Handling personal data

22.1 Computers or mobile devices with storage capacity (e.g. memory sticks or smart phones), which contain personal data that if lost could cause damage or distress to individuals must not be taken outside Estyn offices unless **encrypted** and/or capable of having data wiped remotely.

22.2 The Data Protection Act and GDPR requires that **all personal data** is handled in a secure manner so care must also be taken if you take any personal data, which is less sensitive or voluminous than that defined in Appendix 1 of Estyn's Information Assurance Policy as protected personal data, outside Estyn premises on a laptop or mobile device.

22.3 The policy on personal data handling is summarised thus:

Level of sensitivity	**Level of protection**
Official – personal data	May not be removed from Estyn without approval and should be stored on encrypted device
Sensitive data, e.g. Official – inspection (draft reports, etc.)	May be removed from Estyn premises. Preferably, should be stored on encrypted device but, for practical reasons, a non-

	encrypted device (e.g. USB stick) may be used with extra care taken to avoid loss.
Data which if lost is unlikely to cause damage or distress – e.g. information is already in the public domain or would be released under a Freedom of Information request	May be removed from Estyn premises without encryption

Please contact the ITSO if you are in any doubt about how to apply the policy relating to personal data.

22.4 Where staff are using unencrypted laptops, e.g. for presentations, then data should be held on a memory stick and either run from the stick, or transferred to the desktop and run from there. Where they are run from the desktop they should be deleted at the end of the session and the Recycle bin should be emptied. This should be standard practice when using unencrypted equipment to avoid any risk of data leakage.

22.5 Hard-copy sensitive information must not be removed from offices without management approval (at Assistant Director level or above).

22.6 Any loss or theft of equipment or information must be reported to the IT Security Officer immediately.

23 Classified information and protective markings

23.1 All information (including records held electronically) must be classified in accordance with the UK Government's Protective Marking Scheme – more information on how and when to apply protective markings is included in Estyn's Information Assurance Policy.

23.2 When sending protectively marked email you must include 'OFFICIAL' (followed by the relevant category) in the subject line and also at the start of the message so that the recipient knows that they need to take care when handling the email content.

24 Removable media

24.1 Removable media devices, such as USB data sticks, required for Estyn business purposes must be obtained through Office Services.

24.2 You must not attach or attempt to attach any device to the Estyn ICT systems that has not been approved through the ITSO.

24.3 Data held on removable media storage devices such as CD or USB data stick is vulnerable to loss. Such devices are also a ready source of virus transmission. Care must be taken to assess any risks associated with the transfer of data onto Estyn ICT systems via removable media. Contact the ITSO if you are unsure.

24.4 If a media storage device contains a protectively marked document, then special care must be taken when required to use it inside an insecure environment. The principle here is to never attach to an unclassified / third party network.

24.5 If using you are using infrared and/or Bluetooth devices on any Estyn equipment, please be mindful that there are increased risks of interception.

24.6 Smartphone users must follow the security guidance provided when the device was issued.

25 Breaches of the ICT usage policy

25.1 Breach of this policy may result in disciplinary action and possible dismissal.

25.2 Potential breaches of this policy which come to the attention of management will be investigated by the Human Resources team and the ITSO. The Human Resources team is responsible for taking the lead in any disciplinary proceedings arising from a breach of these rules by staff. Where disciplinary action is considered necessary, all action will be undertaken formally. Estyn staff should refer to the Discipline Policy and the formal action section of the Discipline Procedures.

25.3 An investigation into an allegation of a breach of this policy will only be made if there is reasonable suspicion that a breach has occurred. The investigation may involve such steps as accessing emails or other information stored on or communicated using the ICT systems and this might include consideration of a user's Internet usage.

25.4 The user will be informed at an appropriate time that such steps have been taken in relation to him/her together with an explanation of the reasons why those steps were taken. Once an investigation has been completed, if appropriate, the investigating officers will destroy copies of any evidence they have collected.

25.5 Estyn will co-operate fully with the police or government officials of an appropriate level in any investigation relating to unlawful activities conducted using the organisation’s ICT equipment or systems. If the investigation proves that material has been accessed that is pornographic, advocates illegal acts, violence or discrimination, this will be considered gross misconduct and appropriate disciplinary procedures will be followed.

25.6 In all cases of illegal acts, the police will be notified. Evidence may be disclosed to the police, where there is reasonable suspicion of criminal activity.

25.7 The ICT Service Desk and ITSO must be informed immediately an IT security breach is suspected or detected. Staff should also speak to their line manager or the Human Resources team, or they may under Estyn's Whistleblowing policy inform one of the officers designated there.

26 Possible offences

26.1 Breaches of this policy can result in charges of misconduct or gross misconduct. The result of such disciplinary charges being proven can vary from an informal/formal warning to dismissal. However, each case shall be considered on its merits. A decision on an appropriate penalty should the allegation(s) of a breach be proven, would be taken based on the particular circumstances of the case and the level of seriousness of the offence, whether minor, serious or gross-misconduct.

27 Misconduct

27.1 The following list of activities, which is not exhaustive, provides examples of conduct considered to breach acceptable ICT usage. These would normally lead to disciplinary action such as a formal/informal warning:

i. introducing a virus or causing disruption to normal ICT service through reckless system use;
ii. divulging your password or demanding a colleague share their password with you;
iii. introducing material which infringes copyright;
iv. disregarding standards of storage, transmission or disposal of information e.g. storing personal movies, inappropriate graphics/image files, animations or games;
v. sending email or other electronic transmission which interferes with your official duties, or might embarrass Estyn.
vi. unauthorised installation of software - whether downloaded from the Internet or introduced from disk, CD or other media;
vii. sending chain mail, unsolicited "spam" or indiscriminate communication;
viii. canvassing, lobbying or propagation of personal opinions such as political or religious beliefs;
ix. making false claims or denials regarding the use of Estyn systems; and
x. misuse of social media (see Estyn's Social Media Policy and Guidelines for further information).

28 Gross misconduct

28.1 These are deliberate activities which constitute a major breach of conduct in the use of ICT, bringing Estyn into disrepute and/or making any further working relationship or trust between Estyn and the employee impossible. Examples include:

i. excessive personal use of email or the Internet at the expense of the interests of Estyn;
ii. downloading, accessing, emailing or otherwise introducing material that causes offence to colleagues or contravenes Estyn policies such as the Equal Opportunities Policy;
iii. using Estyn systems to commit fraud or other illegal/criminal activity;
iv. falsifying records, such as logs, email or other electronic transmission;
v. downloading, accessing or otherwise deliberately introducing sexually explicit/obscene media into Estyn;
vi. introduction of software intending to cause damage to Estyn systems;
vii. using email or other electronic transmission to communicate deliberately threatening or inciting material;
viii. hacking (attempting to bypass or subvert system security controls) or otherwise deliberately obtaining unauthorised access to corporate systems or other user accounts;
ix. theft of equipment, data or other property belonging to Estyn, including personal property stolen from Estyn offices;
x. logging on as another user or accessing any ICT systems that you have not been given permission to access; and
xi. serious misuse of social media (see Estyn's Social Media Policy and Guidelines for further information).

29 Glossary

Application Systems	A program or set of programs that support a business process. Examples within Estyn include – IRIS Accounts System, Cygnum, Judgement Form System, a set of Excel spreadsheets or Inspection Outcomes Database
Bluetooth	A radio standard for short distance communication between electronic devices without using wires. It can be used to connect, for example, computers, mobile phones, ear-pieces, etc.
C: Drive	See Hard Disk (drive)
Device	General term for a piece of ICT equipment (see hardware)
Downloading	Electronically extracting and saving files from a network or the internet to the computer you are using
Encryption	The process of converting data into a coded form to prevent it from being read and understood by an unauthorized party
Hard disk (drive)	Computer storage device, generally fitted inside a PC or laptop – often referred to as the C: Drive
Hardware	Physical components of a computer system, e.g. printer, monitor etc. Often referred to as devices
ICT Service Desk	This is your first port of call for all issues and enquiries surrounding ICT use within Estyn (support@westgateit.com).
Infrared	This is a standard for short distance communication similar to Bluetooth although perhaps not as mobile.
Macro	In computer science, a set of instructions for performing a task automatically
Network	For the purposes of this document the ‘Estyn network’ is defined as any device connected to Estyn servers or processors by whatever means, encrypted or not
Phishing	This is an attempt to obtain sensitive information such as usernames, passwords, and credit card details, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication
Ransomware	This is a type of malicious software from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

Remote Access Key Fobs	More accurately termed the “Secure ID Token” – this is a small handheld device that displays a constantly changing number. A user must enter this number as well as their username and password in order to gain remote access.
Removable Media	Refers to data storage devices that can be inserted into a computer in order to access/store files – e.g. CD, DVD or USB memory stick.
Software	A set of computer programmes and instructions that perform a task
Spam	The practice of bulk emailing unsolicited messages.
Trojans	Trojans are virus programs that are hidden within legitimate looking files. They are activated inadvertently - for example by opening an infected email attachment or downloading and running a file from the Internet.
USB Devices	USB (Universal Serial Bus) is a standard “plug-in” interface between a computer and add-on devices (such as cameras, scanners, keyboards, printers, etc.). With USB, a new device can be added to your computer without having to add an adapter card or even having to turn the computer off.
Virus	A computer virus is a small program written to alter the way a computer operates, without the permission or knowledge of the user.
Worms	Worms are virus-like programs that replicate themselves from system to system over a computer network. They often require no human interaction to be able to replicate them.
Y: Drive	Network file storage area associated with a unique user account.

Appendix A: Frequently asked questions

Personal use of Estyn ICT systems

Q1. Can I store personal photos or media files on my computer or the network?
A1. *Personal images, movies, video, films, animation, games or music files should not be stored on an Estyn computer or network as such files can take up a great deal of storage space and lengthen the time/cost of file backups. This storage space is for official records and work related personal information only and therefore Estyn reserves the right to remove any personal files without notice.*

Q2. Can I use the Internet for personal online shopping?
A2. *Yes, but this must only be done during non-working time and on the Estyn guest wifi.*

Q3. I've got some games on that I want loaded onto my PC. How do I go about loading them?
A3. *You must not load them onto your PC – only business software authorised by the ITSO will be allowed on Estyn ICT systems. Unauthorised software will be removed and disciplinary proceedings may be taken against the employee(s) concerned.*

Email

Q1. A member of staff is off sick, how do I get access to their email and Y: Drive?
A1. *You must submit a request via your line manager to the IT Service Desk stating the business justification for accessing another's personal account. You should be aware that access is not automatically granted and may be refused.*

Q2. A member of staff is off sick, how do I reset their out of office message?
A2. *You must submit a request via the IT Service Desk stating why the change is required and the form of words for the message.*

Q3. Can I use email for personal use?
A3. *Yes - but only in non-working hours unless there is an urgent need, for example to deal with a domestic emergency. All personal emails must be sent with the personal email disclaimer attached and, like personal telephone calls, should be kept within reasonable limits. The increasingly large volume of email can have a detrimental effect on network performance and even small messages, in sufficiently large quantities can use up valuable storage space if not deleted promptly.*

Q4: The rules state that 'excessive' personal use of email is now considered gross misconduct. What constitutes excessive personal use in this case?
A4: *Excessive personal email or Internet activity is defined as being usage 'at the expense of Estyn' – i.e. personal email or Internet use that conflicts with the business needs of the organisation. Whilst the rules suggest a definition of 'reasonable'*

personal use of email (no more than a handful of messages a week), it is for individual line managers to decide whether their employees are using email or the Internet in a way that adversely affects their performance. Similarly, excessive personal use of the online text facilities of Skype is discouraged; this should be for work-related communications only.

Q5: I want to ask a friend to meet up for coffee; can I send them an email?
A5: *Yes, but in this case it would be better to make a brief telephone call or text message. If you do use email, make sure you delete any such ephemeral messages as soon as possible.*

Q6. Can I access personal/web email accounts (e.g. Hotmail)?
A6. *Only in cases where the line manager authorises, but generally not if the connection to the internet is via the Estyn network. Use of such accounts leaves us open to virus attack. Any queries please speak to the ITSO for advice.*

Q7: The ICT Usage Rules state that I can use the Internet for online shopping during non-working time, but that I must not use my Estyn email address for buying or selling items. I'm confused. How can I continue to shop online if I can't use my email address?
A7: *When shopping online, your email address is used for contact purposes only – e.g. to confirm a transaction or as a means of contacting you if the item(s) you require are out of stock. When shopping online, if prompted to enter an email address, you should use a personal email address.*

Q8: I have used my Estyn email address for online shopping in the past and now find that I get regular newsletters from companies. What should I do?
A8: *The rules state that you must not use your Estyn email address as a contact point when buying or selling personal items. Receiving an email communication from a company you may have dealt with in the past, does not in itself constitute buying or selling. However, the rules do advise that you reduce the amount of personal email you receive at work. Therefore, you should change your subscription settings so that such emails are delivered to your personal address rather than your work one. If this is not possible, then you should simply delete the email once you have read it.*

Remote working

Q.1 I am working away from the office, can I automatically send my email to a non-Estyn email account?
A2. *No, it could result in the inadvertent forwarding of confidential information or technical difficulties.*

Q2. Can I work at home on my own PC?
A2. *This is not recommended as the security and integrity of home PCs cannot be guaranteed. Only unmarked data can be worked on and strict criteria must be followed; the anti-virus, anti-spyware, personal firewall and operating system software must be up to date and information must be depersonalised and deleted after use. It is preferable to borrow a pool laptop for occasional use; provision for more regular use can be made via the Flexible working policy and Guidance on*

home-working, which also defines eligibility for a PC for home use. See para 6.2 pf policy regarding use of Terminal Services.

Q3. Can I use my Internet connection at home to access the Estyn network?
A3. *You can access Estyn systems from home but only if you are using an Estyn laptop or are doing so as part of a Disaster Recovery or business continuity exercise using a Terminal Services client. However in order to access our systems via your own Internet connection a technology called VPN is required, together with an RSA encryption token and a client running on your Estyn laptop.*

Q4. Can I access my email or other Estyn internal network applications from an internet cafe?
A4. *Yes. This can be down by logging in to the terminal server. This uses a VPN to provide a sercure connection.*

Usernames and passwords

Q1. I am about to go away on holiday. Can I give my password to a colleague so that they are able to check for important emails while I am absent?
A1. *No. Your password is part of your identity and as such must not be divulged to another person (you would not lend someone your driving license to drive your car, or your passport to go on holiday!). You should enable your Out-of-office Assistant. You may also give your colleague access to your inbox* ***through his/her account****, if appropriate. You can arrange this via the IT Service Desk prior to your departure.*

Q2. If another person logs on to and stores personal files on my computer, will I be blamed if they are found on my machine?
A2. *No. The username of the person who saved the image is associated with the file. This is why you must never share your username/password with anyone else because you are accountable for all activity that takes place under your username*.

Network security

Q1. Why are a number of administrative functions locked down on my desktop?
A1. *Many administrative features include the ability to navigate the network and make changes which may introduce security risks. Functions have been locked down to prevent staff making accidental changes and also to allow the machine to be supported more easily and efficiently. This is normal practice in large corporate ICT environments such as ours.*

Q2. Why is my access to some Internet sites blocked?
A2. *Principally, to protect staff from inadvertently accessing offensive sites. Some sites can be unblocked on request but these are dealt with on a case-by-case basis and depend on business need. If you would like to make a request to unblock a site you should log an email request via the IT Service Desk.*

Q3. Can I download software from the Internet?
A3. *No – downloading software leaves us open to virus attack and could have possible copyright or licensing implications. There are also issues around software taking up capacity on our servers, which is needed to store official information. New software can impact on other services that are being provided, therefore all software must be approved and impact tested prior to loading onto the Estyn network. If the software is required for business purposes you must contact the IT Service Desk.*

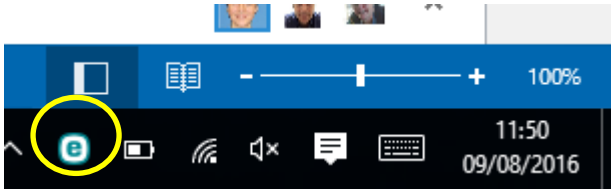
Q4. Can I use USB ports for digital cameras, memory sticks etc.?
A4. *There are a number of security risks to consider when using USB devices, in particular memory sticks. Estyn laptops are updated with virus checking software regularly but to minimise the risks of contamination only Estyn memory sticks should be attached where possible. There may be a need to attach a digital camera or mobile phone from time to time, e.g. to retrieve evidence photographs, but these instances should be kept to an absolute minimum. In event of query, please contact ITSO.*

Q5. I have a personal phone that makes use of Infrared and Bluetooth. Can I connect it to my laptop?
A5. *No. Only devices procured through Estyn arrangements can be connected to Estyn laptops. Use of Bluetooth and Infrared must be cleared by the ITSO.*

Q6. Am I able to access our systems via wireless?
A6. *Within the office we have a local wireless network known as Estyn and also an Estyn Guest network, for which the access key to visitors can be supplied on request. On other wireless systems (including your own at home) you will require the user's permission and a valid access key. All of our traffic will be encrypted via RSA technology and the link will be set up using the client that exists on your desktop.*

Q7. I've got a CD with some new software on which I need for business purposes. What should I do with it?
A7. *All requests for the installation of new software must be made via the IT Service Desk. All software must be impact tested and approved prior to loading onto the network. We will also require a valid license check.*

Q8. How do I virus check removable media?
A8. *Individual files are automatically checked as each is accessed and opened. However, it is good practice to check the complete device using the Virus Scan provisions in the ESET software on your laptop. This can be run at any time. Right click on the ESET logo in your system tray (see below).*



Q9. A friend/relative has emailed me with a warning about a virus. What should I do?
A9. *Forward the email onto the ITSO and IT Service Desk*.

Q10. I want to download an app to my Estyn smartphone. What procedure should I follow?

A10. *This will depend on two things. Does the app have a valid business use and is it a free or paid app. The request should be routed to ITSO if there will be a cost to Estyn or if there would be business benefits from sharing details of the app with colleagues. Guidance on how to download apps is available here.*

Protecting information

Q1. I've heard that I can take personal data outside the office but only on an 'encrypted device' – how do I know if I have one of those?
A1. *A 'device' in this sense refers to any piece of mobile ICT equipment, which is capable of storing data (e.g. laptops, memory sticks or mobile phones). Currently the only devices that are encrypted are usb drives and laptops. Be aware though that certain types of personal data might be considered so sensitive, that they cannot be removed from the office without prior authorisation from the IT Security Officer, even on an encrypted device. If in doubt, seek the advice of the ITSO or your Assistant Director.*

Q2. Estyn maintains a number of datasets containing personal information. I sometimes need to work off-site. Is it OK to take a copy of the data I need with me?
A2. *There are restrictions in place on the movement of personal data, which are based on the level of sensitivity of the information and whether accidental loss or compromise would be likely to cause damage or distress to the individuals concerned. As a general rule, data which falls into the class of 'protected' personal data cannot be removed from the office unless authorised by the IT Security Officer. Data not classed as 'protected' but which nevertheless could cause harm to an individual if accidentally released may be taken off-site, but only on an encrypted device (see above). There are currently no restrictions on the movement of personal data whose loss would not cause damage or distress to individuals.*

Q3: I have received a document marked 'Commercial in Confidence' from another organisation. How should I treat it?
A3: *You should apply an equivalent protective marking that is appropriate to the document's content. Most commercially sensitive material would be assigned a marking of PROTECT – Commercial. For more information on the use of government protective markings, see Estyn's Information Assurance Policy.*

Q4. Can I use my C: Drive to store information?
A4. *Yes, but this drive is not backed up to the server so you risk losing this data. It is recommend that you use use your Y:Drive or personal space in Sharepoint to ensure such information is brought into a backup regime and to minimise the risk of data leakage.*

Q5: Do I have to lock my laptop away if I leave my desk at lunchtime or for a meeting?

A5: *Laptops must be locked away at the end of the working day so that they remain secure overnight when the risk of theft is likely to be highest. If you leave your desk during the working day, you do not need to secure your laptop unless it is likely that you will be absent for the remainder of the day.*

Appendix B: Email and Internet – Do's and Don'ts

Do

- Try to restrict the use of email and Internet to official business
- Start or end personal email with the standard disclaimer
- Obtain confirmation of receipt for important emails sent
- Check your email daily or arrange for an authorised person to do so
- Activate the 'Out of Office Assistant' when absent from office
- Reply promptly to all email messages requiring a reply, or if not possible send an acknowledgement of receipt with estimate of timing of a more comprehensive response
- Refer any suspect emails or files to the ITSO for checking

Don't:

- Attempt to circumvent security systems or procedures
- Apply incorrect protective security markings to data
- Access pornography or other inappropriate material via the Internet at any time
- Share personal passwords so that others can log on as you
- Use anyone else's password or allow others to use yours
- Download software without permission
- Transmit copyrighted material without permission
- Send email to the press
- Post information to interactive websites
- Publish material to interactive websites
- Subscribe to any non work related bulletin boards, newsgroups or any other internet related information posting service
- Open email attachments containing software applications without first seeking advice from ITSO
- Send email containing pornography or potentially criminal material
- 'Spam' internet users via the Estyn Internet system
- Impersonate any other person when using email or amend messages received
- Send emails to large user groups ('all staff', 'all HMI', etc.) unless absolutely necessary and there is not a more appropriate form of communication, e.g. SharePoint Announcements, Works Matter, etc.)
- Add new recipients into email 'strings' without considering whether it is appropriate for them to see the whole content or better to begin a new 'string'
- Make excessive personal use of the internet, including Skype instant messaging, during work time

Please refer to Appendix C for further guidance on the effective use of email.

Appendix C: Guidelines on the effective use of email

These guidelines are intended to help you make efficient and effective use of email. By following the advice given, you will be able to establish efficient practices for handling email and avoid many potential pitfalls.

Managing your email

Email is an essential means of communication. However, if you don't manage your email use, it can be a drain on your productivity and become stressful.

Constantly flicking to your email as new messages arrive can be very disruptive to your working day. If an incoming email message distracts you from productive work, it takes an average of four minutes to get back on track. So in one day, if 15 emails derail you, you've lost an hour of productive time. By establishing efficient practices for dealing with email, you can take control of your working day:

1 Wherever possible talk instead of type! It is easy to overuse email to communicate. It is often quicker and more valuable to walk and talk to the individuals concerned or to pick up the phone.
2 Managers should be careful not to encourage unhealthy expectations – staff should not feel that they must respond to emails immediately, out of hours, when on leave, etc., unless it is part of their role.
3 Clear out your inbox – it reduces clutter and stress. Don't store emails in your inbox. Move them into folders. A cluttered inbox risks items being overlooked, missed or forgotten. It is also stressful to open you inbox at the beginning of the day to hundreds of messages. By keeping a clear inbox you can take charge of your day and your work priorities.
4 Avoid any folder becoming too large. Large folders are difficult to manage and are slow to open. Carry regular housekeeping to remove messages that you no longer require.
5 Manage when you check your email. Make sure you check your email as frequently as is required to carry out your role but try to set specific time aside to deal with email so that you can have blocks of time when you can work on other operational or strategic work without interrupting your productive flow. For example, you might choose to check your email five or six times a day. You might want to consider switching off any desktop pop-ups or sound alerts when new messages arrive, so that you can gain more control over your working day.
6 Try to avoid using email for urgent matters. Regularly flagging messages as urgent creates an environment in which people feel they must view each email as it arrives. This creates an unpredictable and inefficient working day. Use the "three hour" rule – for anything that requires a response within three hours use more alternative communication methods such as telephone or in person.

New messages

1 Use informative subject lines – and use appropriate protective markings (see information assurance policy). When starting a new message, make effective

and appropriate use of the subject. It is important that recipients of your messages have a good indication as to which messages to read first and which ones can be read at a later date. It is also easier to find relevant messages at a later date.

2 Stick to one topic per email. Several short messages are usually preferable to one long message covering many separate subjects.
3 Be clear about any points of action. When you send a message to someone that requires an action, make it very clear within the first few lines of the e-mail what is expected. If possible, you should also include a due date.
4 Avoid overuse of capital letters. Capital letters can be used sparingly to emphasise a word or phrase. If they are used excessively then this is the email equivalent of shouting.
5 Ensure that you are emailing the correct address! Check any auto-completed addresses are for the intended recipient – there might be several similar 'first names' stored.
6 Use mailing lists rather than trying to maintain your own list and having a large number of individual addresses as recipients.
7 Use proper spelling, grammar and punctuation. This is important because poor spelling, grammar and punctuation may give a bad impression of Estyn and will not help you to clearly convey your message. Messages with no full stops or commas are difficult to read and in extremes can sometimes distort the meaning of your text. Outlook has facilities for checking your spelling which you should make use of.
8 Follow the Estyn rules for email signatures.

Replying

1 Think before you hit "reply-all". Ask yourself whether all of the people on the recipient list really need to see your reply. Many times people are added to an e-mail thread and get included in all of the subsequent discussions which occur. This can be a major inconvenience for some of the recipients.
2 Pause before you hit the Send button. If you are angry or upset about the message you are replying to, give yourself some time to calm down before replying. Reading through your reply several times will also help. Sending a quick and angry response rarely helps and often leads to an increasingly acrimonious exchange of messages.
3 Paste responses to common queries. If you are frequently asked the same questions then save the text of your responses so you can paste it into subsequent replies. Alternatively, consider proving the information on SharePoint and then send your recipient the link (URL).
4 Take care when replying to email lists. When you receive a message from an email list, be very careful to direct your reply to the appropriate address. A common problem arises when a person should reply to an individual, but instead sends that reply to the entire list.

Forwarding

1 Add a summary to put the forwarded message in context. When forwarding messages consider including a summary at the beginning. This will allow the

new recipient to determine what has already been discussed. It will also allow you to include the actions or information specific to that person so that he/she can quickly provide the response you require.

2 Legal obligations. Never send or forward messages containing libellous, defamatory, offensive, discriminatory or obscene remarks.

3 Never forward virus hoaxes and chain letters. If you receive a message warning you of a virus that will damage your PC, it is almost certainly a hoax. Sometimes virus hoaxes actually contain viruses themselves! By forwarding hoaxes you will waste valuable resources and will not be help any of the recipients. Email chain letters usually promise untold riches or ask for your support for a charitable cause. Even if the message seems to be legitimate, the name of the senders is often forged . If such a message seems to be too good to be true, it probably is! It is therefore sensible to just delete such messages.

Attachments

1 Be very careful when opening attachments, even if the message appears to be from someone you know. Email attachments infected with viruses are one of the most widely used methods for infecting PCs.

2 Be selective in the sending of attachments. Wherever possible, either include the text in the body of the email or even better save the file in SharePoint and then send the link to your recipient.

3 Consider the file format of the attachment. When sending an attachment you should ensure, in advance, that the recipient can handle your attachment – remember, not all computer users use the same software. For example, a user external to Estyn might not have the latest version of Word installed whilst other organisations may have a policy which discourages the sending or receiving of certain file types.

4 Be careful about the size of an attachment. If you really do need to add attachments, think carefully about the file size. Files in text (txt), revisable text format (rtf) and portable document format (pdf) are usually more compact formats than files in Word (doc) format. Office 2016 file formats, for example docx, are more compact than the doc format, although you will need to take care that the person you are sending the file to can open files that are in Office 2016 format. Images in documents can result in very large file sizes.

Legal issues

1 Email policy and regulations, including misuse of email, are detailed within the main text of the ICT security and usage policy.

Data Protection – The General Data Protection Regulations 2016 applies to computerised records and this includes email. It is important that staff do not retain email messages containing any personal information for longer than that information is required. The length of time an email with personal data should be retained is dependent upon the purposes for which the information was obtained. Once this purpose is complete, the email should be deleted. For further information please see the Information Assurance policy on our website.